Christopher I. Brain
cbrain@tousley.com
Kim D. Stephens
kstephens@tousley.com
Tousley Brain Stephens PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Tel: 206.682.5600
Fax: 206.682.2992

Interim Lead Plaintiffs' Counsel

Keith S. Dubanevich
kdubanevich@stollberne.com
Steve D. Larson
slarson@stollberne.com
Stoll Stoll Berne Lokting & Shlachter P.C.
209 SW Oak Street
Portland, Oregon 97204
Tel: 503.227.1600
Fax: 503.227.6840

Interim Liaison Plaintiffs' Counsel

[Additional counsel appear on the signature page.]

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

IN RE: PREMERA BLUE CROSS CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates to All Actions	Case No. 3:15-md-2633-SI **PLAINTIFFS' CONSOLIDATED CLASS ACTION ALLEGATION COMPLAINT** **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

Page

Plaintiffs Mary Fuerst, Ross Imbler, Anne Emerson, Debbie Hansen-Bosse, William Fitch, Eric Forseter, Anne Michelle Blackwolfe, Krishnendu and Madhuchanda Chakraborty, Howard Kaplowitz, Stuart and Ilene Hirsh, Darin Purcell, Kevin Smith and Catherine Bushman, Sharif Ailey, April Allred, Elizabeth Black, Ralph Christopherson, Robert and Theresa Foulon, Crystal Hayes, Barbara Lynch, Kevin McLallen, Surya Prakash, Gabriel and Laura Webster, and Joann Welch, individually and on behalf of the proposed Classes defined below, allege as follows upon personal knowledge, experience, information and belief, including investigation conducted by their attorneys.

I. NATURE OF THE CASE

1. Plaintiffs bring this class action lawsuit against Premera because of its failure to protect the confidential information of millions of consumers—including their names, dates of birth, mailing addresses, telephone numbers, email addresses, Social Security numbers, member identification numbers, medical claims information, financial information, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Sensitive Information").

2. Premera is one of the largest healthcare benefits companies in the Pacific Northwest and is also a participant in the national Blue Cross Blue Shield Association (which offers healthcare to consumers throughout the United States and its territories, covering more than 105 million Americans). Premera's participation in the Blue Cross Blue Shield Association provides its members with access to healthcare providers throughout the country and provides non-Premera Blue Cross members (referred to as "Blue members") with access to its network.

3. In order to become a Premera member (or, for Blue members, receive healthcare services from a provider within the Premera network), an individual must give Premera his or her Sensitive Information. Plaintiffs and the putative class took reasonable steps to preserve the

confidentiality of their Sensitive Information in many ways, including protecting the Sensitive Information with confidential passwords and relying upon physician-patient privilege and confidentiality. Premera maintains this Sensitive Information in a centralized database.

4. As a healthcare insurance provider, Premera is required to protect both its members' and also Blue members' Sensitive Information, including by adopting and implementing specific data security regulations and standards set forth under HIPAA.

5. In addition to its implied statutory obligation, Premera expressly promises—throughout its Notice of Privacy Practices, Code of Conduct, public statements, and other written understandings—to safeguard and protect Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards.

6. Unfortunately, Premera's failure to protect the Sensitive Information resulted in one of the largest healthcare data breaches in history. On March 17, 2015, Premera revealed that its computer network had been breached and the Sensitive Information of approximately 11 million of its former and current members, Blue members, and employees was compromised.

7. According to Premera, the breach started in May 2014 and went undetected for nearly one year. Worse yet, after discovering the breach, Premera waited months before notifying all affected individuals.

8. The breach not only revealed that Premera failed to provide the level of data protection that it promised and that members paid for, it also exposed millions of individuals' Sensitive Information to an increased risk of misuse by unauthorized third parties (e.g., identity theft). In fact, affected individuals face a particularly real risk of misuse here (i.e., to the extent their information hasn't been misused already) because their Sensitive Information was specifically targeted by hackers seeking to steal consumer data. Many of the class members have

already suffered medical fraud, tax fraud, credit card fraud, and phishing scams, as a result of Premera's illegal conduct. All class members are in real and imminent danger of the same fate.

9. Had Premera informed members that it would use inadequate security measures, consumers (like Plaintiffs and the members of the Classes) would not have been willing to sign-up or pay for Premera's healthcare benefits at the price charged, if at all.

10. Premera's failure to implement adequate security protocols jeopardized millions of consumers' Sensitive Information, fell well short of its statutory and professional standard obligations, and diminished the value of the services provided by it. (In other words, because Premera failed to disclose its gross security inadequacies, it delivered a fundamentally less useful and less valuable service than the one members paid for).

11. Accordingly, Plaintiffs bring suit, on behalf of themselves and all others similarly situated, to seek redress for Premera's unlawful conduct.

II. PARTIES

12. Plaintiff Mary Fuerst is a natural person and citizen of the State of Alaska. Plaintiff Fuerst brings this action on behalf of herself and the Nationwide and Alaska Classes, as defined below.

13. Plaintiff Ross Imbler is a natural person and citizen of the State of Alaska. Plaintiff Imbler brings this action on behalf of himself and the Nationwide and Alaska Classes, as defined below.

14. Plaintiff Anne Emerson is a natural person and citizen of the State of Arkansas. Plaintiff Emerson brings this action on behalf of herself and the Nationwide and Arkansas Classes, as defined below.

15. Plaintiff Debbie Hansen-Bosse is a natural person and citizen of the State of California. Plaintiff Hansen-Bosse brings this action on behalf of herself and the Nationwide and California Classes, as defined below.

16. Plaintiff William Fitch is a natural person and citizen of the State of Idaho. Plaintiff Fitch brings this action on behalf of himself and the Nationwide and Idaho Classes, as defined below.

17. Plaintiff Eric Forseter is a natural person and citizen of the State of Maryland. Plaintiff Forseter brings this action on behalf of herself and the Nationwide and Maryland Classes, as defined below.

18. Plaintiff Anne Michelle Blackwolfe is a natural person and citizen of the State of Massachusetts. Plaintiff Blackwolfe brings this action on behalf of herself and the Nationwide and Massachusetts Classes, as defined below.

19. Plaintiffs Krishnendu & Madhuchanda Chakraborty are natural persons and citizens of the State of Maryland. Plaintiffs Chakraborty bring this action on behalf of themselves and the Nationwide and Maryland Classes, as defined below.

20. Plaintiff Howard Kaplowitz is a natural person and citizen of the State of New Jersey. Plaintiff Kaplowitz brings this action on behalf of himself and the Nationwide and New Jersey Classes, as defined below.

21. Plaintiffs Stuart and Ilene Hirsh are natural persons and citizens of the State of Oregon. Plaintiffs Hirsh bring this action on behalf of themselves and the Nationwide and Oregon Classes, as defined below.

22. Plaintiff Darin Purcell is a natural person and citizen of the State of Oregon. Plaintiff Purcell brings this action on behalf of himself and the Nationwide and Oregon Classes, as defined below.

23. Plaintiffs Kevin Smith and Catherine Bushman are natural persons and citizens of the State of Tennessee. Plaintiffs Smith and Bushman bring this action on behalf of themselves and the Nationwide and Tennessee Classes, as defined below.

24. Plaintiff Sharif Ailey is a natural person and citizen of the State of Texas. Plaintiff Ailey brings this action on behalf of himself and the Nationwide and Texas Classes, as defined below.

25. Plaintiff April Allred is a natural person and citizen of the State of Washington. Plaintiff Allred brings this action on behalf of herself and the Nationwide and Washington Classes, as defined below.

26. Plaintiff Elizabeth Black is a natural person and citizen of the State of Washington. Plaintiff Black brings this action on behalf of herself and the Nationwide and Washington Classes, as defined below.

27. Plaintiff Ralph Christopherson is a natural person and citizen of the State of Washington. Plaintiff Christopherson brings this action on behalf of himself and the Nationwide and Washington Classes, as defined below.

28. Plaintiffs Robert & Theresa Foulon are natural persons and citizens of the State of Washington. Plaintiffs Foulon bring this action on behalf of themselves and the Nationwide and Washington Classes, as defined below.

29. Plaintiff Crystal Hayes is a natural person and citizen of the State of Washington. Plaintiff Hayes brings this action on behalf of herself and the Nationwide and Washington Classes, as defined below.

30. Plaintiff Barbara Lynch is a natural person and citizen of the State of Washington. Plaintiff Lynch brings this action on behalf of herself and the Nationwide and Washington Classes, as defined below.

31. Plaintiff Kevin McLallen is a natural person and citizen of the State of Washington. Plaintiff McLallen brings this action on behalf of himself and the Nationwide and Washington Classes, as defined below.

32. Plaintiff Surya Prakash is a natural person and citizen of the State of Washington. Plaintiff Prakash brings this action on behalf of himself and the Nationwide and Washington Classes, as defined below.

33. Plaintiffs Gabriel & Laura Webster are natural persons and citizens of the State of Washington. Plaintiffs Webster bring this action on behalf of themselves and the Nationwide and Washington Classes, as defined below.

34. Plaintiff Joann Welch is a natural person and citizen of the State of Washington. Plaintiff Welch brings this action on behalf of herself and the Nationwide and Washington Classes, as defined below.

35. Defendant Premera Blue Cross is a healthcare benefits provider existing under the laws of the State of Washington with its headquarters and principal place of business located at 7001 220th Street SW, Building 1, Mountlake Terrace, Washington 98043. Premera's relevant operations, including its primary marketing, administration and information security operations, as well as its vital employees (such as its Chief Information Security Officer) are all located in

the State of Washington. Premera is also registered to conduct business in the State of Oregon (Oregon Secretary of State Registry Number 447360-80) and Alaska (Premera Blue Cross of Alaska, which is a trade name only).

III. JURISDICTION AND VENUE

36. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Classes is a citizen of a state different from Defendant, and (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

37. This Court has personal jurisdiction over Defendant because it is registered to and regularly does conduct business in this District, and the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated, in part, from this District.

38. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated from this District. Venue is additionally proper because Defendant is registered to and does conduct business in this District.

IV. FACTUAL BACKGROUND

A. Premera Had a Duty to Protect its Members' Sensitive Information From Unauthorized Disclosures.

39. Based on obligations created by HIPAA, based on industry standards, based on specific governmental warnings to Premera about its failure to meet those obligations, and based on the promises it made to its members, Premera had an obligation to keep its members' Sensitive Information confidential and to protect it from unauthorized disclosures. Class members provided their Sensitive Information to Premera with the common sense understanding

that Premera would comply with its obligations to keep it confidential and secure from unauthorized disclosures.

40. Premera admitted its duty to keep the Sensitive Information confidential and secure through its own statements. Through its Notice of Privacy Practices (which all members receive), Premera promised to keep members' Sensitive Information confidential and protect it from unauthorized disclosure. For instance, the Notice of Privacy Practices appearing on Premera's primary website states, in relevant part:[1]

> **THE PRIVACY OF YOUR MEDICAL AND FINANCIAL INFORMATION IS VERY IMPORTANT TO US.**
>
> At Premera Blue Cross, we are committed to maintaining the confidentiality of your medical and financial information, which we refer to as your "personal information," regardless of format: oral, written, or electronic.
>
> * * *
>
> **OUR RESPONSIBILITIES TO PROTECT YOUR PERSONAL INFORMATION**
>
> Under both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act, Premera Blue Cross must take measures to protect the privacy of your personal information. In addition, other state and federal privacy laws may provide additional privacy protection. Examples of your personal information include your name, Social Security number, address, telephone number, account number, employment, medical history, health records, claims information, etc.
>
> We protect your personal information in a variety of ways. For example, we authorize access to your personal information by our employees and business associates only to the extent necessary to conduct our business of serving you, such as paying your claims. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to discipline if they violate them. Our privacy policy and practices apply equally to personal information about current and former

[1] *Premera Notice of Privacy Practices*, Premera Blue Cross, *available at* https://www.premera.com/wa/visitor/privacy-policy/ (last visited Oct. 6, 2015).

> members; we will protect the privacy of your information even if you no longer maintain coverage through us.
>
> We are required by law to:
>
> - protect the privacy of your personal information;
> - provide this Notice explaining our duties and privacy practices regarding your personal information;
> - notify you following a breach of your unsecured personal information; and
> - abide by the terms of this Notice.

41. Premera recognized the importance of keeping consumers' Sensitive Information private and repeatedly promised to protect that information and comply with the data security requirements mandated by, among other things, federal and state privacy laws. For instance, in its Code of Conduct, Premera stated[2]:

> We are committed to complying with federal and state privacy laws, including the HIPAA privacy regulations, that protect financial and health information of our customers. We use the following privacy principles to guide our actions:
>
> Customers – Customers should enjoy the full array of privacy protections afforded to them by law and routinely granted by their providers. This is a values-based approach whereby we are focused on two core values: Customer Care and Integrity.
>
> * * *
>
> We are committed to ensuring the security of our facilities and electronic systems to prevent unauthorized access to Premera's and our customers' protected personal information (PPI).
>
> We are expected to be aware of and follow established corporate policies, processes and procedures that are designated to secure our buildings and electronic systems in compliance with HIPAA Security requirements.

42. Premera's data security obligations were particularly important given the substantial increase in healthcare-related data breaches in recent years. Premera's failure to comply with those obligations was particularly egregious in light of governmental warnings

[2] *Premera Code of Conduct 2014*, Premera Blue Cross, *available at* http://premera.com/documents/030553.pdf (last accessed Oct. 6, 2015).

regarding the possibility of hacker attacks. Such warnings further established Premera's duty to keep the Sensitive Information private and secure.

43. On April 8, 2014—just one month before the Premera breach—the Federal Bureau of Investigation's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise."[3]

44. Worse yet, a couple weeks before the at-issue breach, the U.S. Office of Personnel Management directly notified Premera about its network security vulnerabilities.[4] The U.S. Office of Personnel Management's April 18, 2014 report revealed that Premera failed to implement adequate measures to secure its network. It found "several areas of concern related to Premera's network security controls" and noted that "patches are not being implemented in a timely manner," "a methodology is not in place to ensure that unsupported or out-of-date software is not utilized," and a vulnerability scan identified "insecure server configurations."[5]

---

[3] *(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014), FBI Cyber Division Private Industry Notification, *available at* http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf.

[4] Mike Baker, Feds Warned Premera About Security Flaws Before Breach, Seattle Times, Mar. 18, 2015, *available at* http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/ (last visited Oct. 6, 2015).

[5] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, Audit of Information Systems General and Application Controls at Premera Blue Cross (Nov. 28, 2014), https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/opm-audit.pdf.

45. Federal auditors notified Premera weeks before the breach that its network-security procedures were inadequate and informed it that some of the vulnerabilities could be exploited by hackers and expose sensitive information.[6]

B. The Data Breach Revealed—For The First Time To the Public—That Premera Failed To Properly Protect Consumers' Sensitive Information.

46. On May 5, 2014, hackers began the initial attack on Premera's servers. A "phishing" email was sent to a Premera employee falsely purporting to be from a Premera Information Technology (IT) employee. The email included instructions to download a "security update." Premera's employee downloaded this "update," which was actually malware that allowed hackers access to Premera's servers.

47. Notably, various internal security assessments that Premera had undertaken prior to this period confirmed that it was vulnerable to this type of attack.

48. The hackers used the domain name in their email of "premrera.com" (i.e., using an additional "r"). This wrong domain was visible in the email message. Around this same time, another phishing domain of "prennera.com" was also registered.

49. After the Premera employee downloaded the malware, hackers had access to at least two of Premera's servers for many months completely undetected.

50. In October 2014, Premera engaged Mandiant, a cyber-security firm, to perform an assessment of the security of its network. Mandiant provided its Mandiant Intelligent Response (MIR) agents (a tool to identify indicators of compromise and malware) to install on Premera's workstations and laptops for the purposes of scanning for malware and other infections.

---

[6] Mike Baker, *Feds Warned Premera About Security Flaws Before Breach*, Seattle Times, *available at* http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/ (Oct. 6, 2015).

51. The pilot phase of the project began in December 2014 and continued until early January 2015. During this time, Premera began installing MIR agents on workstations and laptops. Premera did not install network sensors until January 28, 2015.

52. On January 29, 2015, Mandiant discovered a signature for SOGU malware traffic on the Premera network, confirmed infection of two servers, and confirmed that the malware was "beaconing" to attacker sites. By January 30, 2015, Premera had uncovered that the SOGU malware had been in its system since May 2014.

53. In February 2015, Mandiant continued to try to understand the full extent of the breach and the whether and how much information had been removed from Premera's system. At this time, Premera finally agreed to deploy Mandiant's agents on all Premera servers, workstations, and laptops in order to assess the scope of the breach. This installation was only complete in late February, nearly a month after Premera first discovered that a breach had occurred.

54. On February 20, 2015, Premera notified the FBI of the data breach. On February 25, 2015, the FBI met with Premera and Mandiant. The FBI began its own investigation, as well.

55. Premera chose not to inform the public of the breach at this time although it had sufficient knowledge of the extent and scope of the breach, deciding instead to further investigate and attempt to remediate the breach before letting the public know that their Sensitive Information had been stolen (and was continuing to be stolen).

56. Premera further waited until the weekend of March 6-8 to perform the complete remediation of its network, during which time information was still being accessed and stolen. Mandiant continued to monitor the network for the following week to ensure Premera had completely cleansed its system.

57. It wasn't until March 17, 2016—46 days after first learning of the breach—that Premera finally revealed to the public and governmental authorities that a massive data breach had occurred.

58. In its notice, Premera revealed that its computer network was the target of "a sophisticated attack to gain unauthorized access to [its] Information Technology (IT) systems."[7] As a result, the Sensitive Information belonging to approximately 11 million consumers—including its current and former members, employees, and other Blue members—was compromised. The breach affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and affiliate brands Vivacity and Connexion Insurance Solutions, Inc. The breach also affected members of other Blue Cross Blue Shield plans who sought treatment in Washington, Oregon or Alaska.

59. Premera eventually acknowledged that the breach actually started in May 2014 and went undetected by it for nearly one year.[8]

60. One month before Premera announced the Sensitive Information had been breached, another major healthcare provider reported that hackers had successfully taken sensitive information of approximately eighty million consumers. Security researchers believe that attackers initially gained access to the databases containing that information through phishing attempts (i.e., using legitimate-looking emails or websites to trick individuals into revealing confidential information, such as database login credentials) and linked malware[9] involved in those phishing attacks to Chinese hackers who authorities refer to as "Deep Panda."

---

7 *Premera Has Been The Target Of A Sophisticated Cyberattack*, Premera Blue Cross, *available at* http://premeraupdate.com/ (last visited Oct. 6, 2015).

8 *Id.*

9 "Malware" refers to malicious software designed to infiltrate and damage computers or computer systems.

61. Malware thought to have been authored by Deep Panda was later discovered in connection with the phishing website www.prennera.com.

C. Premera Violated HIPAA and Industry Standard Data Protection Protocols.

62. HIPAA requires that healthcare providers (like Premera) adopt administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of consumers' Sensitive Information.

63. Unfortunately, Premera's data breach resulted from a variety of failures to follow HIPAA mandated data-security protocols, many of which are also industry standard. Among such deficient practices, Premera's breach shows that it failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training on phishing attempts, adequate intrusion detection systems, regular reviews of audit logs and authentication records, and other similar measures to protect the confidentiality of the Sensitive Information it maintained in its data systems.

64. More specifically, Premera's security failures demonstrate that it failed to honor its duties by failing to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber attacks;

b. Protect Plaintiffs' and the Classes' Sensitive Information adequately;

c. Ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. Ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4); and

j. Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and

appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b).

65. Had Premera implemented the above-described data security protocols, the consequences of the data breach could have been avoided, or at least significantly reduced (as the breach could have been detected nearly one year earlier, the amount of Sensitive Information compromised could have been greatly reduced, and affected consumers could have been notified—and taken protective/mitigating actions—much sooner). For instance, had Premera (i) adequately trained its employees to protect themselves against phishing attempts (like those attempts described in Paragraphs 60-63 above), (ii) implemented adequate security protocols to detect breaches (i.e., detecting unauthorized access to its databases), or (iii) adequately reviewed authentication logs for anomalies (e.g., detecting abnormal access to its databases from unknown locations, or accessing or transferring large amounts of Sensitive Information), the breach could have been identified and thwarted before considerable amounts of Sensitive Information were compromised.

66. Setting aside the fact that major healthcare entities (like Premera) have been targeted in damaging hacking attempts in recent years, Premera was specifically warned that its network-security procedures were inadequate and that some of the vulnerabilities could be exploited by hackers to expose sensitive information (as previewed above). Premera thus knew or should have known that a data breach would likely result from its deficient security and privacy practices described above.

67. Even though its members both expected and paid for the above-described security measures as part of their insurance premiums (i.e., that HIPAA-mandated and industry standards

would have been used to protect their Sensitive Information), they were not adequately implemented (if at all), which resulted in the unauthorized release of their Sensitive Information.

D. It is Well Established That Security Breaches Lead to Instances of Identity Theft.

68. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as SSNs to open financial accounts, receive government benefits and incur charges and credit in a person's name.[10] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

69. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[11]

70. According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[12] Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[13]

---

10 *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* http://www.gao.gov/new.items/d07737.pdf.

11 *Id.*

12 *See Identity Theft*, Federal Trade Commission, http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Oct. 6, 2015).

13 The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

71. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit various types of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.[14] Further, loss of private and personal health information can expose the victim to loss of reputation, loss of job employment, blackmail and other negative effects.

72. Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Sensitive Information directly on various Internet websites making the information publicly available. In one study, researchers found hundreds of websites displaying stolen Sensitive Information. The study concluded:

73. It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[15]

---

[14] *See Identity Theft*, Federal Trade Commission, *available at* http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Oct. 6, 2015).

[15] *See The Underground Credit Card Blackmarket*, StopTheHacker, *available at*

74. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[16] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[17] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

75. Further, medical databases are particularly high value targets for identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[18] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

76. In fact, individuals whose information was compromised in a similar data breach by the same hackers—Deep Panda—have already fallen victims to identity theft, such as tax return fraud.[19]

77. Indeed, Premera's own data breach notification statements recognize the long-lasting harmful effects of its misconduct and recommends that affected individuals remain

---

http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited Oct. 6, 2015).

[16] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), http://news.cnet.com/8301-27080_3-10460902-245.html (last visited Oct. 6, 2015).

[17] *Id.*

[18] *See Study: Few Aware of Medical Identity Theft Risk*, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited Oct. 6, 2015).

[19] *See* Jose Pagliery, *A Hacker Stole Our $3,500 Tax Refund*, CNN Money (Apr. 15, 2015), http://money.cnn.com/2015/04/15/technology/tax-hacker/ (last visited Oct. 6, 2015).

vigilant to the possibility of fraud and identity theft by indefinitely reviewing their credit card, bank, and other financial statements for unauthorized activity.

E. Plaintiffs' Experiences Underscore the Fact That All Class Members are in Imminent Danger of Identity Theft.

ALASKA

78. Plaintiff Mary Fuerst is a resident of Fairbanks, Alaska and was an Alaska resident during the period of the Premera Breach. Plaintiff Fuerst was a Premera policyholder from 2008 to 2013 and made partial premium payments under that policy through her employer. In or around March 2015, Plaintiff Fuerst received a letter from Premera notifying her that her personal information may be compromised. Starting around the same time, she began receiving phishing calls seeking her personal information. Prior to the Premera breach she had not received calls of this nature. Soon thereafter, a fraudulent international charge appeared on Plaintiff Fuerst's debit card. Although her bank ultimately reimbursed her for the fraudulent charge, Plaintiff Fuerst had to obtain a replacement card and complete a fraud affidavit. Plaintiff Fuerst has spent about 20 hours to date addressing issues arising from the Premera Breach.

79. Plaintiff Ross Imbler is a resident of Fairbanks, Alaska and was an Alaska resident during the period of the Premera Breach. Plaintiff Imbler has been a Premera policyholder since 2011 and makes partial premium payments through his employer. In or around March 2015, Plaintiff Imbler received three letters from Premera indicating that his, his wife's, and his then 2-year-old daughter's personal information may be compromised. Plaintiff Imbler is especially concerned about the long-term threat of identity theft to his daughter, as well as the immediate threat of fraud and identity theft for him and his wife. Plaintiff Imbler has spent about six hours to date addressing issues arising from the Premera Breach.

ARKANSAS

80. Plaintiff Anne Emerson is a resident of Little Rock, Arkansas and was an Arkansas resident during the period of the Premera Breach. Plaintiff Emerson has been an Arkansas Blue Cross Blue Shield ("AR BCBS") policyholder since 2004 and makes partial premium payments under that policy through her spouse's employer. Plaintiff Emerson received medical treatment in Washington State between 2004 and 2007. In or around March 2015, Plaintiff Emerson received a letter from AR BCBS notifying her that her personal information may have been compromised in the Premera Breach. Concerned that she would be the victim of fraud and/or identity theft, Plaintiff Emerson purchased credit monitoring and identity theft prevention that costs her approximately $100 annually. Plaintiff Emerson has spent about five hours to date addressing issues arising from the Premera Breach.

CALIFORNIA

81. Plaintiff Debbie Hansen-Bosse is a resident of San Clemente, California and was a California resident during the period of the Premera Breach. Plaintiff Hansen-Bosse and her two 14-year-old daughters have been Premera insureds since 2007. In or around March 2015, Plaintiff Hansen-Bosse received a letter from Premera notifying her that her and her daughters' personal information may have been compromised. In or around May 2015, while monitoring her credit, Plaintiff Hansen-Bosse discovered a hard inquiry for an auto loan on her credit report that she did not recognize and has been unable to verify as legitimate. Also in and around May 2015, Plaintiff Hansen-Bosse's checking account was fraudulently accessed, causing failed automatic payments for two months of credit card payments. Concerned that she would be the victim of fraud and/or identity theft, Plaintiff Hansen-Bosse purchased credit monitoring and identity theft prevention that costs her approximately $25 per month. Plaintiff Hansen-Bosse has spent about 30 hours to date addressing issues arising from the Premera Breach.

IDAHO

82. Plaintiff William Fitch is a resident of Rigby, Idaho and was an Idaho resident during the period of the Premera Breach. Plaintiff Fitch was a Blue Cross of Blue Shield of Idaho policyholder from 1995 to 2013 and made partial premium payments through his employer. In or around March 2015, Plaintiff Fitch received a letter from Premera notifying him that his personal information may have been compromised. Starting around the same time, he began receiving phishing calls and emails seeking his personal information. Prior to the Premera breach he had not received these suspicious solicitations. Plaintiff Fitch has spent about 30 hours to date addressing issues arising from the Premera Breach.

MARYLAND

83. Plaintiff Eric Forseter is a resident of Bethesda, Maryland and was a Maryland resident during the period of the Premera Breach. Plaintiff Forseter was a Premera policyholder from 2008 to May 2015 and made partial premium payments through his employer. In or around March 2015, Plaintiff Forseter received a letter from Premera notifying him that his personal information may have been compromised. On or around May 1, 2015, a criminal fraudulently charged approximately $2,000 in airline tickets and office furniture on Plaintiff Forseter's credit card account. Although his financial institution ultimately reversed the fraudulent charges, Plaintiff Forseter had to wait for a replacement card and reset automatic bill payments for at least 25 accounts with the new card number. Plaintiff Forseter has spent about 20 hours to date addressing issues arising from the Premera Breach.

MASSACHUSETTS

84. Plaintiff Anne Michelle Blackwolfe is a resident of Shrewsbury, Massachusetts and was a Massachusetts resident during the period of the Premera Breach. Plaintiff Blackwolfe has been a Premera policyholder since 2009 and makes partial premium payments through her

employer. In or around March 2015, Plaintiff Blackwolfe received a letter from Premera notifying her that her personal information may have been compromised. Plaintiff Blackwolfe has spent about 25 hours to date addressing issues arising from the Premera Breach.

85. Plaintiff Krishnendu & Madhuchanda Chakraborty are residents of Burlington, Massachusetts and were Massachusetts residents during the period of the Premera Breach. Mr. Chakraborty was a Premera policyholder, with Mrs. Chakraborty as a dependent insured, for approximately six months in 2012 and made partial premium payments through his employer. In or around March 2015, the Chakrabortys received a letter from Premera notifying them that their personal information may have been compromised. In and around June 2015, Mrs. Chakraborty had unauthorized online music charges on her credit card account. Although her bank ultimately reversed the fraudulent charges, she had to wait for a new credit card and temporarily lost access to her line of credit. The Chakrabortys have spent about fifteen hours to date addressing issues arising from the Premera Breach.

NEW JERSEY

86. Plaintiff Howard Kaplowitz is a resident of Livingston, New Jersey and was a New Jersey resident during the period of the Premera Breach. Plaintiff Kaplowitz has been a Premera policyholder since about 2012 and makes partial premium payments through his employer. In or around March 2015, Plaintiff Kaplowitz received a letter from Premera notifying him that his personal information may have been compromised. Plaintiff Kaplowitz has spent about ten hours to date addressing issues arising from the Premera Breach, including monitoring his credit report for fraudulent activity.

OREGON

87. Plaintiffs Stuart & Ilene Hirsh are residents of Salem, Oregon and were Oregon residents during the period of the Premera Breach. Mr. Hirsh was a Premera policyholder, with

Mrs. Hirsh as a dependent insured, from approximately 1999 to 2006 and made partial premium payments through his federal employment. In or around March 2015, Mr. and Mrs. Hirsh received letters from Premera notifying them that their personal information may have been compromised. Mr. and Mrs. Hirsh have spent about six hours to date addressing issues arising from the Premera Breach, including monitoring their credit reports for fraudulent activity.

88. Plaintiff Darin Purcell is a resident of Milwaukie, Oregon and was an Oregon resident during the period of the Premera Breach. Plaintiff Purcell has been a Premera policyholder since 2013 and makes partial premium payments through his employer. In or around March 2015, Plaintiff Purcell received a letter from Premera notifying him that his personal information may have been compromised. Plaintiff Purcell has spent about three hours to date addressing issues arising from the Premera Breach, including monitoring his credit report for fraudulent activity.

TENNESSEE

89. Plaintiffs Kevin Smith and Catherine Bushman, husband and wife, are residents of Franklin, Tennessee and were Tennessee residents during the period of the Premera Breach. Plaintiffs Smith and Bushman were both Premera policyholders at various times from approximately 2005 to 2010, then approximately 2011 to 2013, and each made partial premium payments through their employer. In or around March 2015, Plaintiffs Smith and Bushman received letters from Premera notifying them that their personal information may have been compromised. Also in and around March 2015, Plaintiffs Smith and Bushman received a large IRS tax refund check despite having not yet filed their 2014 tax return. After contacting the IRS, they discovered that someone had filed a fraudulent tax return using their names and Social Security numbers. Plaintiffs Smith and Bushman then filed identity theft affidavits with the IRS and the FTC, a police report, and identity credit watch with one of the credit bureaus. At an in-

person appointment with the IRS in Nashville, they were informed that, going forward, they will have to manually submit their tax returns with a security PIN. The processing of their 2014 tax return and refund was delayed approximately four months. In or around July of 2015, a criminal attempted to fraudulently open a credit card in both of their names, but the bank called Plaintiffs Smith and Bushman and they were able to confirm the fraud and cancel the account. Plaintiffs Smith and Bushman have spent about 30 hours each to date addressing issues arising from the Premera Breach.

TEXAS

90. Plaintiff Sharif Ailey is a resident of Keller, Texas and was a Texas resident during the period of the Premera Breach. Plaintiff Ailey has been a Premera policyholder since November 2011 and makes partial premium payments through his employer. In or around March 2015, Plaintiff Ailey received a letter from Premera notifying him that his personal information may have been compromised. In or around June 2015, Plaintiff Ailey discovered fraudulent credit accounts were being opened in his name. He has spent approximately $100 requesting credit reports, freezing his credit report, and attempting to remove the fraudulent activity from his credit report. As a result of these credit issues caused by the Premera Breach, Plaintiff Ailey was unable to refinance the mortgage on his house. Plaintiff Ailey has spent about 25 hours to date addressing issues arising from the Premera Breach.

WASHINGTON

91. Plaintiff April Allred is a resident of Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Allred and her son were Premera insureds from 2007 to 2009 and from 2011 to 2012, and her husband, the policyholder, made partial premium payments through his employer. In or around March 2015, Plaintiff Allred received a letter from Premera notifying her that her and her family's personal information may have been

compromised. On or about April 15, 2015, Plaintiff Allred's 2014 income tax return was rejected due to the use of her son's Social Security number in another fraudulently filed return. Plaintiff Allred had to take additional trips to her accountant's office, submit her tax return manually by mail, and wait several weeks longer to receive her tax refund. Plaintiff Allred has spent about 25 hours to date addressing issues arising from the Premera Breach, including monitoring her credit report and bank accounts for fraudulent activity.

92. Plaintiff Elizabeth Black is a resident of Seattle, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Black was a Premera policyholder from 2000 to 2005 and made partial premium payments through her employer. On or about February 18, 2015, Plaintiff Black received a cellular phone that she never ordered, with an order date of February 13, 2015. On or about February 23, 2015, she learned that four additional cellular phones were fraudulently purchased in her name at two different retail locations in Oregon. On or about February 20, 2015, Plaintiff Black received a debit card for which she never applied. After speaking with the various vendors and indicating that these accounts were fraudulently opened, Plaintiff Black learned that the personal information used to open the accounts included her name, date of birth, mailing address, and Social Security number. After contacting the vendors multiple times, speaking with their fraud departments, and filing police reports, she was able to cancel the accounts. Plaintiff Black had to take time off from work without pay to tend to these problems, in addition to time spent at work on the phone trying to mitigate and resolve the identity theft and fraud. In or around March 2015, Plaintiff Black finally received a letter from Premera notifying her that her personal information may have been compromised. Plaintiff Black has spent about 25 hours to date addressing issues arising from the Premera Breach, including checking her credit report and bank accounts for fraudulent activity.

In addition, Plaintiff Black also spent approximately $70 in unreimbursed overnight postage to place security freezes on her credit report.

93. Plaintiff Ralph Christopherson is a resident of Seatac, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Christopherson has been a Premera policyholder since 2011 and makes partial premium payments through his employer. In or around March 2015, Plaintiff Christopherson received a letter from Premera notifying him that his personal information may have been compromised. On or about April 2, 2015, Plaintiff Christopherson was the victim of a phishing scam: a man called, claiming he could help fix his computer, and he already had Plaintiff Christopherson's Social Security number and some old credit card numbers. After getting remote access to Plaintiff Christopherson's computer, the criminal fraudulently accessed Plaintiff Christopherson's bank account to steal approximately $900 via Western Union. He is still in the process of seeking reimbursement for this fraud. Plaintiff Christopherson has spent about 80 hours to date addressing issues arising from the Premera Breach, including placing credit locks on his bank account and credit reports, attempting to resolve the fraudulent charges, and monitoring his accounts for additional fraud.

94. Plaintiffs Robert & Theresa Foulon are residents of Bellevue, Washington and were Washington residents during the period of the Premera Breach. Mr. Foulon has been a Premera policyholder, with Mrs. Foulon and their children as dependent insureds, from approximately 1992 to 2009, then 2010 to present. Mr. Foulon now makes premium payments through his self-employment; prior to 2009 he made partial premium payments through his employer. In or around March 2015, the Foulons received letters from Premera notifying them that their and their children's personal information may have been compromised. In or around April 2015, they then received a letter from the IRS indicating that their $9,539 tax refund was

processing even though they had not yet filed a return. After logging into his tax account and seeing the bank account destination for the direct deposit was not theirs, Mr. Foulon contacted the IRS and reported that the tax return was fraudulent. The Foulons had to fill out the necessary forms to report the fraud and file their actual tax return manually, which they will always have to do going forward. On or about September 14, 2015, they received another letter from the IRS verifying that the prior return was fraudulent and providing a PIN for future filings. Mr. Foulon is still attempting to sort out his family's 2014 tax return due to this attempted identity theft. The Foulons have spent about 30 hours to date addressing issues arising from the Premera Breach, including monitoring their credit reports for additional fraudulent activity.

95. Plaintiff Crystal Hayes is a resident of Lynnwood, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Hayes has been a Premera policyholder since 2012 and makes partial premium payments through her employer. In or around March 2015, Plaintiff Hayes received a letter from Premera notifying her that her personal information may have been compromised. Soon after the breach notification, her credit cards were cancelled and reissued due to fraudulent activity, but Plaintiff Hayes was unaware of the cancellation and her cards were declined when she attempted to use them. She had to reset her automatic bill payments with the reissued card information as well. Plaintiff Hayes has spent about five hours to date addressing issues arising from the Premera Breach, including requesting and checking her credit report and bank statements for fraudulent activity.

96. Plaintiff Barbara Lynch is a resident of Seattle, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Lynch has been a Premera policyholder for approximately 17 years and makes premium payments through her employer. Starting in and around January 2015, numerous fraudulent credit inquiries appeared on

Plaintiff Lynch's credit report, causing her credit score to drop approximately 100 points. Soon thereafter, she received notification from three different financial institutions that fraudulent accounts were opened in her name. Concerned that she would be the victim of additional fraud and/or identity theft, Plaintiff Lynch immediately purchased credit monitoring and identity theft protection, which costs her $30 per month. In or around March 2015, Plaintiff Lynch received a letter from Premera notifying her that her personal information may have been compromised. Plaintiff Lynch estimates that she has spent over 100 hours to date addressing issues arising from the Premera Breach, including aggressive remedial measures to restore her credit score. She continues to receive fraud alerts to the present day.

97. Plaintiff Kevin McLallen is a resident of Covington, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff McLallen has been a Premera policyholder since approximately 2011 and makes partial premium payments through his employer (and now through COBRA). In or around March 2015, Plaintiff McLallen received a letter from Premera notifying him that his personal information may have been compromised. In or around April 2015, fraudulent charges appeared on Plaintiff McLallen's credit and debit cards for small charges in New Jersey and Michigan. Even more recently, Plaintiff McLallen has received phishing calls where the criminals already have many of his personal identifying information. Plaintiff McLallen has spent about ten hours to date addressing issues arising from the Premera Breach, including pulling credit reports and purchasing his credit scores – and unreimbursed expense – to ensure they were accurate. He also spent time calling his banks to notify them of the fraudulent activity and researching additional credit security services.

98. Plaintiff Surya Prakash is a resident of Seattle, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Prakash was a Premera policyholder

from 2005 to 2012 and made partial premium payments through his employer. In or around December 2014, approximately $3,500 in fraudulent charges appeared on his bank account. Plaintiff Prakash immediately notified the bank and canceled the account, but was without access to the stolen funds for two weeks until reimbursement. In or around February 2015, he again experienced fraudulent activity totaling approximately $250 on different bank accounts. Again, Plaintiff Prakash canceled the cards and had to wait a few weeks for reimbursement of the stolen funds. In or around March 2015, Plaintiff Prakash received a letter from Premera notifying him that his personal information may have been compromised. In or around August 2015, Plaintiff Prakash received a letter from a collections company indicating he purchased over $2,000 in plane tickets that he never purchased. He has contacted all three credit bureaus to place alerts and freezes on his credit report. Plaintiff Prakash has spent about five hours to date addressing issues arising from the Premera Breach, including monitoring his bank accounts and credit report for additional fraud.

99. Plaintiffs Gabriel & Laura Webster are residents of Seattle, Washington and were Washington residents during the period of the Premera Breach. Mr. Webster has been a Group Health and Regents Blue Cross policyholder, with Mrs. Webster and their 12-year-old son as dependent insureds, from approximately 2009 to 2011 and 2012 to present, respectively. Mr. Webster made premium payments on these policies through his employer, and the Websters all received medical treatment in Washington State from 2009 to present. In or around November 2014, Mr. Webster had fraudulent charges on his credit card. Although these charges were ultimately reimbursed, he temporarily lost access to his line of credit. In or around February 2015, the Websters attempted to file their 2014 tax return but were prevented from doing so due to a fraudulent return already filed in their names. They had to pay their accountant an extra fee

to submit an amended filing and had to manually file the tax return. Going forward, the Websters will have to file their taxes using a new security PIN provided to them by the IRS every year. In or around March 2015, the Websters received letters from Premera notifying them that their and their son's personal information may have been compromised. The Websters have spent about 25 hours to date addressing issues arising from the Premera Breach, including numerous hours on the telephone attempting to resolve the fraudulent tax return.

100. Plaintiff Joann Welch is a resident of Moses Lake, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Welch has been a Blue Cross of Illinois policyholder for over a decade and makes partial premium payments through her former employer's retirement plan. She has received medical treatment in Washington State for the past 25 years. In or around March 2015, Plaintiff Welch received a letter from Premera notifying her that her personal information may have been compromised. Around the same time as the breach notification, she received an automated phishing call seeking her personal information and referencing her former employer. Prior to the Premera breach she had not received any such suspicious calls. Plaintiff Welch has spent about four hours to date addressing issues arising from the Premera Breach, including ordering and checking her credit report for fraudulent activity.

V. CLASS ALLEGATIONS

A. Nationwide Data Breach Class

101. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3), Plaintiffs assert statutory claims under the Washington Consumer Protection Act (First Claim for Relief) and the Washington data breach notification statute (Second Claim for Relief), and common law claims for negligence (Third Claim for Relief), breach of fiduciary duty (Tenth Claim for Relief), and

misrepresentation by omission (Eleventh Claim for Relief) on behalf of a nationwide class defined as follows:

> **Nationwide Data Breach Class**: All persons in the United States whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015.

i. Nationwide Premera Policyholder Subclass

102. Plaintiffs Fuerst, Imbler, Emerson, Kunz, Fitch, Gregory, Forseter, Blackwolfe, Chakraborty, Kaplowitz, Hirsh, Purcell, Bushman, Ailey, Allred, Black, Christopherson, Foulon, Hayes, Lynch, McLallen, Prakash, Webster, and Welch assert their common law claims for breach of express contract (Fourth Claim for Relief), breach of implied contract (Fifth Claim for Relief), and unjust enrichment (Sixth Claim for Relief) on behalf of a nationwide subclass defined as follows:

> **Nationwide Premera Policyholder Subclass:** All Nationwide Data Breach Class members who paid money to Premera prior to March 17, 2015 in exchange for health insurance.

103. As alleged herein, Premera's headquarters are in Mountlake Terrace, Washington, its data centers and servers are located in Washington, and the Premera employees responsible for making decisions with respect to data security are based in Washington. Premera's conduct resulting in the data breach took place exclusively, or primarily, in Washington. Premera, being headquartered in Washington, would reasonably expect to be bound by the laws of Washington. Furthermore, the majority of the Nationwide Data Breach Class members are residents of the state of Washington.[20] Accordingly, applying Washington law to the claims of the Nationwide Data Breach Class and Nationwide Premera Policyholder Subclass is appropriate.

[20] http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html

B. Alternate Statewide Common Law Classes

104. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3), and in the alternative to the common law claim for negligence asserted on behalf of the Nationwide Data Breach Class, Plaintiffs assert their common law claim for negligence (Third Claim for Relief) on behalf of separate statewide classes defined as follows:

> **Statewide [name of State] Common Law Classes:** All residents of [name of State] whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015.

i. Statewide Premera Policyholder Subclasses

105. Plaintiffs Fuerst, Imbler, Emerson, Kunz, Fitch, Gregory, Forseter, Blackwolfe, Chakraborty, Kaplowitz, Hirsh, Purcell, Bushman, Ailey, Allred, Black, Christopherson, Foulon, Hayes, Lynch, McLallen, Prakash, Webster, and Welch assert their common law claims for breach of contract (Forth Claim for Relief), breach of implied contract (Fifth Claim for Relief), unjust enrichment (Sixth Claim for Relief), and misrepresentation by omission (Eleventh Claim for Relief) on behalf of separate statewide subclasses defined as follows:

> **Statewide [name of State] Premera Policyholder Subclasses:** All residents of [name of State] whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015, and who paid money to Premera prior to March 17, 2015 in exchange for health insurance.

C. Alternate Statewide Statutory Classes

106. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3), and in the alternative to the statutory claims asserted on behalf of the Nationwide Data Breach Class, Plaintiffs Emerson, Hansen-Bosse, Fitch, McKenzie, Gregory, Forseter, Blackwolfe, Kaplowitz, Hirsh, Purcell, Ailey, Black, Christopherson, Foulon, Hayes, Lynch, McLallen, Prakash, Webster, and Welch assert statutory claims for violation of state consumer protection statutes (Seventh Claim for

Relief) and state data breach notification statutes (Eighth Claim for Relief) on behalf of separate statewide classes, defined as follows:

> **Statewide [name of State] Statutory Classes:** All residents of [name of State] whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015.

107. Plaintiffs Emerson, Hansen-Bosse, Fitch, McKenzie, Gregory, Forseter, Blackwolfe, Kaplowitz, Hirsh, Purcell, Ailey, Black, Christopherson, Foulon, Hayes, Lynch, McLallen, Prakash, Webster, and Welch assert the state consumer protection statute claims (Seventh Claim for Relief) under the consumer protection laws of the following states: Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, Nevada, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Texas, Utah, Vermont, Washington, West Virginia, and Wyoming.

108. Plaintiffs Hansen-Bosse, Kaplowitz, Bushman, Ailey, Allred, Black, Christopherson, Foulon, Hayes, Lunch, McLallen, Prakash, Webster, and Welch assert the state data breach notification law claims (Eighth Claim for Relief) on behalf of separate statewide classes in and under the respective data breach statutes of the following states: California, Illinois, Iowa, Louisiana, Maryland, New Hampshire, New Jersey, North Carolina, South Carolina, Tennessee, Texas, Virginia, and Washington.

109. Plaintiff Hansen-Bosse also asserts claims for violation of the California Confidential Medical Information Act (Ninth Claim for Relief).

110. Excluded from the Classes and Subclass are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and its legal representatives, officers, directors,

assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiffs reserve the right to amend the Class definitions if discovery and further investigation reveal that the Class should be expanded, divided into further subclasses or modified in any other way.

D. Certification of the Proposed Classes and Subclasses is Appropriate.

111. Each of the proposed classes and subclass meets the certification under Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and (b)(3).

112. **Numerosity**: The exact number of members of the Classes is unknown to Plaintiffs at this time, but on information and belief, there are approximately 11 million individuals in the Classes, making joinder of each individual member impracticable. Ultimately, members of the Classes will be easily identified through Premera's records.

113. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include:

a. Whether Defendant failed to safeguard Plaintiffs' and the Classes' Sensitive Information adequately;

b. Whether Defendant failed to protect or otherwise keep Plaintiffs' and the Classes' Sensitive Information secure, as promised;

c. Whether Defendant's storage of Plaintiffs' and the Classes' Sensitive Information in the manner alleged violated HIPAA, federal, state and local laws, or industry standards;

d. Whether Defendant engaged in unfair or deceptive practices by failing to safeguard Plaintiffs' and the Classes' Sensitive Information properly as promised;

e. Whether Defendant violated the consumer protection statutes applicable to Plaintiffs and each of the Classes;

f. Whether Defendant failed to notify Plaintiffs and members of the Classes about the security breach as soon as practical and without delay after the breach was discovered;

g. Whether Defendant acted negligently in failing to safeguard Plaintiffs' and the Classes' Sensitive Information properly;

h. Whether Defendant violated the California Confidential Medical Information Act;

i. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiffs and the members of the each of the Classes, on the other;

j. Whether Defendant's conduct described herein constitutes a breach of its implied or express contracts with Plaintiffs and the members of each of the Classes;

k. Whether Defendant should retain the money paid by Plaintiffs and members of each of the Classes to protect their Sensitive Information; and

l. Whether Plaintiffs and the members of the Classes are entitled to damages as a result of Defendant's conduct.

114. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the Classes. Plaintiffs and the members of the Classes sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

115. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Classes, and have retained counsel competent and experiences in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Classes, and Defendant has no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

116. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Classes.

117. **Policies Generally Applicable to the Classes**: This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiffs and proposed Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Classes, and making final injunctive relief appropriate with respect to the proposed Classes as a whole. Defendant's

practices challenged herein apply to and affect the members of the Classes uniformly, and Plaintiffs' challenge of those practices hinges on Defendant's conduct with respect to the proposed Classes as a whole, not on individual facts or law applicable only to Plaintiffs.

118. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the members of the Classes. The injuries suffered by each individual member of the Classes are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Classes to obtain effective relief from Defendant. Even if members of the Classes could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

VI. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
Violation of the Washington Consumer Protection Act
(On behalf of Plaintiffs, the Nationwide Data Breach Class, and the Nationwide Premera Policyholder Subclass)

119. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

120. Plaintiffs and the Nationwide Data Breach Class are current and former members of Premera or those who received services from healthcare providers in the Premera network and who provided Premera with their Sensitive Information.

121. Washington's Consumer Protection Act, RCW §§ 19.86.010, *et seq.* ("CPA"), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

122. To achieve that goal, the CPA prohibits any person from using "unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce. . . ." RCW § 19.86.020. An unfair or deceptive business practice is one that is likely to deceive a substantial portion of the public or otherwise affect public interest.

123. Defendant expressly promised—throughout its Notice of Privacy Practices, Code of Conduct, public statements, and other written understandings—to safeguard and protect Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards.

124. Defendant failed to disclose that its data security systems and practices were inadequate and did not comport with its expressed promises referenced *supra*, ¶ 138, and otherwise described herein.

125. Defendant's failure to notify Plaintiffs and the Nationwide Data Breach Class promptly about the data breach is unfair because its failure ran contrary to its promised confidentiality practices, exposed Plaintiffs and the Nationwide Data Breach Class to additional (and unnecessary) harm, and otherwise offended public policy.

126. As described throughout this Complaint, Defendant was responsible for securing Plaintiffs' and the Nationwide Data Breach Class's Sensitive Information. Given that it was responsible for creating, overseeing, maintaining, and otherwise implementing its own data security practices, Defendant knew (or should have known) that it was not adequately protecting Plaintiffs' or the Nationwide Data Breach Class's Sensitive Information. Prior to the breach,

neither Plaintiffs, nor members of the Nationwide Data Breach Class, nor the general public knew that Defendant was not implementing adequate data security and privacy protocols. By failing to disclose that it could not and would not protect their Sensitive Information, Defendant actively concealed its true security practices from Plaintiffs and the Nationwide Data Breach Class.

127. Consumers—like Plaintiffs and members of the classes—value their privacy. Companies (such as health insurers) that offer adequate data security protections are more valuable to consumers than those with substandard security practices. As such, consumers will, if given the choice between two otherwise identical services, choose one with adequate security practices over one with substandard security practices.

128. Because of this consumer preference for data security, a healthcare insurance company safeguarding and protecting Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards commands a higher market price for its coverage than a provider with substandard security.

129. Plaintiffs and the Nationwide Premera Policyholder Subclass believed Defendant would adequately protect their Sensitive Information, those security protections were valuable to them, and the protections formed the basis of their bargain inasmuch as Plaintiffs and the Nationwide Premera Policyholder Subclass would not have purchased healthcare insurance from Defendant at the prices charged (if at all) had Defendant disclosed its substandard security practices. Accordingly, Defendant's omission regarding the true protection standard was material.

130. To Plaintiffs and the Nationwide Premera Policyholder Subclass, Defendant's as-promised healthcare insurance offered significantly more utility or value than what was

delivered, which lacked meaningful security protections. Thus, to Plaintiffs and the Nationwide Premera Policyholder Subclass, Defendant's secured healthcare insurance—as promised and paid-for—was substantially more valuable than the unsecure insurance received.

131. Accordingly, had Plaintiffs and members of the Nationwide Premera Policyholder Subclass known that Defendant did *not* actually implement adequate data security protocols, they would not have been willing to purchase its healthcare insurance at the prices charged, if they would have paid money at all.

132. Likewise, had Plaintiffs and members of the Nationwide Data Breach Class known that Defendant did *not* actually implement adequate data security protocols, they would not have been willing to provide Defendant with their Sensitive Information.

133. Defendant's failure to disclose its substandard security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of Plaintiffs' and the Nationwide Class's Sensitive Information. Further, Defendant's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

134. Defendant's unfair acts or practices occurred in its trade or business and has proximately caused injury to Plaintiffs and the putative Nationwide Class. Defendant's general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of its misconduct may last for years (*e.g.*, affected individuals could experience identity theft for years). As a direct and proximate result of Defendant's unfair acts, Plaintiffs and members of the Nationwide Data Breach Class have suffered actual injuries, including without limitation investing substantial time or money in monitoring and remediating the harm inflicted upon them.

135. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people of the State of Washington. The conduct that Plaintiffs challenge directly affects the people of the State of Washington.

136. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Data Breach Class have suffered actual damages, including from the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

137. Further, as a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder Subclass have suffered actual damages in an amount equal to the difference in the market value of the secure healthcare insurance they paid for and the unsecured healthcare insurance they received.

138. Accordingly, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class and Nationwide Premera Policyholder Subclass, seek to enjoin further

violation and recover actual damages and treble damages (where applicable), together with the costs of brining this suit, including reasonable attorneys' fees.

139. With respect to injunctive relief, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class and Nationwide Premera Policyholder Subclass, seek an Order requiring Premera to: (1) engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Premera's systems on a periodic basis, and ordering Premera to correct any problems or issues detected by such third-party security auditors promptly; (2) engage third-party security auditors and internal personnel to run automated security monitoring; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) segment data by, among other things, creating firewalls and access controls so that if one area of Premera's network is compromised, hackers cannot gain access to other portions of Premera's systems; (5) purge, delete, and destroy in a reasonably secure manner Sensitive Information not necessary for its provisions of services; (6) conduct regular database scanning and securing checks; (7) routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) meaningfully educate all class members about the threats they face as a result of the loss of their confidential financial, personal, and health information to third parties, as well as the steps affected individuals must take to protect themselves.

SECOND CLAIM FOR RELIEF
Violation of Washington Data Breach Disclosure Law
(On behalf of Plaintiffs and the Nationwide Data Breach Class)

140. Plaintiffs incorporate all the foregoing factual allegations as if fully set forth herein.

141. Plaintiffs allege additionally and alternatively that RCW § 19.255.010(2) provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *See* RCW § 19.255.010(2) (2005).

142. The data breach described in Section II resulted in an "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant and, therefore, experienced a "breach of [its] security of [its] system", as defined by RCW § 19.255.010(4) (2005).

143. Defendant failed to disclose the breach of its network immediately, after discovering the breach. Instead, it waited months before notifying all affected individuals. Defendant unreasonably delayed informing Plaintiffs and members of the Nationwide Data Breach Class about the data breach after it knew or should have known that the data breach had occurred.

144. Defendant's failure to provide notice immediately after discovering the breach is a violation of RCW § 19.255.010.

THIRD CLAIM FOR RELIEF
Negligence
(On behalf of Plaintiffs and the Nationwide Data Breach Class or, alternatively, the Statewide Common Law Classes)

145. Plaintiffs incorporate all the foregoing factual allegations as if fully set forth herein.

146. Plaintiffs allege additionally and alternatively that Premera required Plaintiffs and Nationwide Data Breach Class members or alternatively, members of the Statewide Common

Law Classes, to submit Sensitive non-public personal health and financial information in order to obtain coverage under a health insurance policy and/or receive treatment in the Blue Cross Blue Shield network.

147. By collecting and storing this data, Premera had a duty of care to use reasonable means to secure and safeguard this personal and health information, to prevent disclosure of the information, and to guard the information from theft. Premera's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give immediate notice in the case of a data breach.

148. Furthermore, given the other major data breaches affecting the healthcare industry and the warnings provided by federal auditors that Premera's network-security procedures were inadequate and that the vulnerabilities could be exploited by hackers and expose sensitive information (as described above), Plaintiffs and the Nationwide Data Breach Class members or alternatively, members of the Statewide Common Law Classes, are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their Sensitive Information stolen.

149. Premera owed a duty to Plaintiff and members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, to provide security consistent with industry standards, statutory requirements, and the other requirements discussed herein, and to ensure that its systems and networks—and the personnel responsible for them—adequately protected its consumers' Sensitive Information.

150. Premera admitted and assumed its duty to implement reasonable security measures as a result of its general conduct, internal policies and procedures, its Privacy Policy, and its Code of Conduct, in which Premera states that it is "committed to ensuring the security of

our facilities and electronic systems to prevent unauthorized access to Premera's and our customers' personal protected information (PPI)." Through these statements, Premera specifically assumed the duty to comply with industry standards and HIPAA in protecting confidential information.

151. Premera's duty to use reasonable security measures arose as a result of the special relationship that existed between Premera and the Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes. The special relationship arose because Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, entrusted Defendant with their confidential data, as part of the health treatment process. Only Premera was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, from a data breach.

152. Premera's duty to use reasonable security measures also arose under HIPAA, pursuant to which Premera is required to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

153. In addition Premera had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by healthcare benefit providers

like Defendant. The FTC publications and data security breach orders described above further form the basis of Premera's duty.

154. Premera's duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because it was bound by, and had committed to comply with, industry standards for the protection of confidential Sensitive Information.

155. Premera breached its common law, statutory and other duties—and thus, was negligent—by failing to use reasonable measures to protect consumers' confidential data from hackers and by failing to provide timely notice of the at-issue breach. The specific negligent acts and omissions committed by Premera include, but are not limited to, the following:

(a) Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and proposed Nationwide Data Breach Class members' or alternatively, members of the Statewide Common Law Classes', confidential data;

(b) Failing to monitor the security of its networks adequately;

(c) Allowing unauthorized access to Plaintiffs' and the proposed Nationwide Data Breach Class members' or, alternatively, members of the Statewide Common Law Classes', confidential data;

(d) Failing to recognize in a timely manner that Plaintiffs' and proposed Nationwide Data Breach Class members' or alternatively, members of the Statewide Common Law Classes', confidential data had been compromised; and

(e) Failing to warn Plaintiffs and the members of the proposed Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, in a timely manner that their Sensitive Information was likely to be and had been compromised.

156. It was foreseeable that Premera's failure to use reasonable measures to protect confidential data, to disclose to Plaintiffs its inadequate security system and to provide timely notice of a breach of such data would result in injury to Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes were reasonably foreseeable, particularly in light of the other major data breaches affecting the healthcare industry and the warning provided by federal auditors (described in Section I, above) that Premera's network-security procedures were inadequate and that the vulnerabilities could be exploited by hackers and expose sensitive information.

157. It was therefore reasonably foreseeable that the failure to safeguard confidential data adequately would result in one or more of the following injuries to Plaintiffs and the members of the proposed Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft

insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

158. Accordingly, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, seek an order declaring that Defendant's conduct constitutes negligence, and awarding them damages in an amount to be determined at trial.

159. Washington law should apply to the negligence claim of the Nationwide Class, or, alternatively, the negligence claims of the Statewide Common Law Classes should be governed by the law of each state in which such state specific claims are brought.

FOURTH CLAIM FOR RELIEF
Breach of Express Contract
(On behalf of Plaintiffs and the Nationwide Premera Policyholder Subclass or, alternatively, the Statewide Premera Policyholder Subclasses)

160. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

161. Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, allege additionally and alternatively that they entered into valid and enforceable contracts with Defendant whereby it promised to provide healthcare and data protection services to them. Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, agreed to, among other things, pay money for such services.

162. Both aspects of Plaintiffs' and the Nationwide Premera Policyholder Subclass members' or alternatively, members of the Statewide Premera Policyholder Subclasses', agreements with Defendant (*i.e.*, the provision of healthcare and data protection services) were material.

163. In its Notice of Privacy Practices, Code of Conduct, public statements, and other written understandings, Defendant expressly promised Plaintiffs and members of Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, to safeguard and protect the confidentiality of their Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards.

164. Defendant promised to comply with all HIPAA regulations, federal, state and local laws, and industry standards to make sure that Plaintiffs' and the Nationwide Premera Policyholder Subclass members' or alternatively, members of the Statewide Premera Policyholder Subclasses', Sensitive Information was protected.

165. These contracts required that Defendant protect Plaintiffs' and the Nationwide Premera Policyholder Subclass members' or alternatively, members of the Statewide Premera Policyholder Subclasses', Sensitive Information and to prevent unauthorized access to such information.

166. Unfortunately, Defendant did not safeguard Plaintiffs' and the Nationwide Premera Policyholder Subclass members' or alternatively, members of the Statewide Premera Policyholder Subclasses', Sensitive Information. Specifically, Defendant did not comply with its promises to abide by HIPAA, federal, state and local laws, or industry standards.

167. The failure to meet these promises and obligations constitutes a breach of express contract.

168. Because Defendant allowed unauthorized access to Plaintiffs' and the Nationwide Premera Policyholder Subclass members' or alternatively, members of the Statewide Premera Policyholder Subclasses', Sensitive Information and otherwise failed to safeguard it as promised, Defendant breached its contracts with Plaintiffs and members of the Nationwide Premera

Policyholder Subclass (or alternatively, members of the Statewide Premera Policyholder Subclasses).

169. A meeting of the minds occurred, as Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, agreed to, among other things, provide Defendant with their accurate and complete information (including their Sensitive Information) and to pay Defendant in exchange for its agreement to, among other things, protect their Sensitive Information.

170. Defendant breached these contracts by failing to implement (or adequately implement) sufficient security measures to protect Plaintiffs' and the Nationwide Premera Policyholder Subclass members' or alternatively, members of the Statewide Premera Policyholder Subclasses', Sensitive Information.

171. Defendant's failure to fulfill its data security and management promises resulted in Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, receiving healthcare insurance that was of less value than they paid for (*i.e.*, healthcare insurance coverage without adequate data security and management practices).

172. Stated otherwise, because Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Premera Policyholder Subclasses, paid for privacy protections (as part of, among other things, their premiums) they did not receive—even though such protections were a material part of their contracts with Defendant—the full benefit of their bargain.

173. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder

Subclasses, have suffered actual damages in an amount equal to the difference in the value of the secure healthcare insurance they paid for and the insecure healthcare insurance they received.

174. Accordingly, Plaintiffs, on behalf of themselves and the other members of the Nationwide Premera Policyholder Subclass, or alternatively, the Statewide Premera Policyholder Subclasses, seek an order declaring that Defendant's conduct constitutes breach of express contract, and awarding them damages in an amount to be determined at trial.

FIFTH CLAIM FOR RELIEF
Breach of Implied Contract
(*In the Alternative to Breach of Express Contract*)
(On behalf of Plaintiffs and the Nationwide Premera Policyholder Subclass or, alternatively, the Statewide Premera Policyholder Subclasses)

175. Plaintiffs incorporate all the foregoing factual allegations as if fully set forth herein, excluding Paragraphs 160-174.

176. Plaintiffs allege additionally and alternatively that in order to benefit from Defendant's insurance coverage, Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, provided Defendant with their Sensitive Information.

177. By providing that Sensitive Information, and upon Defendant's acceptance of such information, Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, on the one hand, and Defendant, on the other, entered into implied contracts whereby Defendant was obligated to take reasonable steps to secure and safeguard that information.

178. Under those implied contracts, Defendant was further obligated to provide Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively,

members of the Premera Policyholder Subclasses, with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

179. Without such implied contracts, Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, would not have provided their Sensitive Information to Defendant.

180. As described throughout, Defendant did not take reasonable steps to safeguard Plaintiffs' and the Nationwide Premera Policyholder Subclass members' or alternatively, members of the Statewide Premera Policyholder Subclasses', Sensitive Information.

181. Because Defendant allowed unauthorized access to Plaintiffs' and the Nationwide Premera Policyholder Subclass members' or alternatively, members of the Premera Policyholder Subclasses', Sensitive Information and failed to take reasonable steps to safeguard that information, Defendant breached its implied contracts with Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Premera Policyholder Subclasses.

182. Defendant's failure to fulfill its data security and management promises resulted in Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, receiving healthcare insurance that was of less value than they paid for (*i.e.*, healthcare insurance coverage without adequate data security and management practices).

183. Stated otherwise, because Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, paid for privacy protections (as part of, among other things, their premiums) they did

not receive—even though such protections were a material part of their contracts with Defendant—the full benefit of their bargain.

184. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, have suffered actual damages in an amount equal to the difference in the value of the secure healthcare insurance they paid for and the insecure healthcare insurance they received.

185. Accordingly, Plaintiffs, on behalf of themselves and members of the Nationwide Premera Policyholder Subclass, or alternatively, the Statewide Premera Policyholder Subclasses, seek an order declaring that Defendant's conduct constitutes breach of implied contract, and awarding them damages in an amount to be determined at trial.

SIXTH CLAIM FOR RELIEF
Restitution/Unjust Enrichment
(On behalf of Plaintiffs and the Nationwide Premera Policyholder Subclass or, alternatively, the Statewide Premera Policyholder Subclasses)

186. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein, excluding Paragraphs 160-174.

187. Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, allege additionally and alternatively that they conferred a monetary benefit on Defendant in the form of fees paid for healthcare insurance. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses.

188. The fees for healthcare insurance that Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder

Subclasses, paid (directly or indirectly) to Defendant were supposed to be used by Defendant, in part, to pay for the administrative costs of data management and security.

189. Defendant did not use such fees to pay for the administrative costs of data management and security.

190. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder Subclass or alternatively, members of the Statewide Premera Policyholder Subclasses, suffered actual damages in an amount equal to the difference in the free-market value of the secure healthcare insurance for which they paid and the insecure healthcare insurance they received.

191. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and members of the Nationwide Premera Policyholder Subclass, or alternatively, the Statewide Premera Policyholder Subclasses, because Defendant failed to implement (or adequately implement) the data management and security measures that they paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

SEVENTH CLAIM FOR RELIEF
Violation of State Consumer Protection Laws
(*In the Alternative to Count I*)
(On behalf of Plaintiffs and the Statewide Statutory Classes)

192. Plaintiffs incorporate all the foregoing allegations as if fully set forth herein, excluding Paragraphs 119-139.

193. Plaintiffs allege additionally and alternatively that the consumer protection laws listed below were enacted to protect consumers by promoting fair competition in commercial markets for goods and services. Specifically, they prohibit unlawful, unfair, deceptive, or fraudulent business acts or practices.

194. As described herein, Defendant has engaged in unlawful, unfair, and deceptive business acts or practices.

195. Based on its statutory and common law obligations, and as admitted and assumed by its own statements, Defendant had a duty to safeguard and protect Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards.

196. In fact, Defendant did not implement adequate security protocols to prevent unauthorized access to Sensitive Information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data breach or otherwise comply with HIPAA data security requirements. Thus, Defendant's conduct was unlawful.

197. As described throughout this Complaint, Defendant was responsible for securing Plaintiffs' and the Statewide Statutory Classes' Sensitive Information. As it was responsible for creating, overseeing, maintaining, or otherwise implementing its own data security practices, Defendant knew (or should have known) that it was not adequately protecting Plaintiffs' or the Statewide Statutory Classes' Sensitive Information. Prior to the breach, neither Plaintiffs, members of the Statewide Statutory Classes, nor the general public knew that Defendant was not implementing adequate data security and privacy protocols. By representing that it could and would protect their Sensitive Information, when it did not in fact do so, Defendant actively concealed its true security practices from Plaintiffs and the Statewide Specific Classes.

198. Consumers—like Plaintiffs and members of the Statewide Statutory Classes—value their privacy. Services (including healthcare insurance) that offer greater data security protections are more valuable to consumers than those with substandard security practices.

Consumers will, if given the choice between two otherwise identical services, choose one with adequate security practices over one with substandard security practices.

199. Because of this consumer preference for data security, a healthcare insurance company safeguarding and protecting Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards commands a higher market price for its coverage than a provider with substandard security.

200. Defendant's failure to disclose its substandard security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of Plaintiffs' and the Statewide Statutory Classes' Sensitive Information. Further, Defendant's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

201. Defendant's unfair acts or practices occurred in its trade or business and have injured a substantial portion of the public. Defendant's general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of its misconduct may last for years (*e.g.*, affected individuals could experience identity theft years later). As a direct and proximate result of Defendant's unfair acts, Plaintiffs and members of the Statewide Statutory Classes have suffered and will suffer actual injuries.

202. Accordingly, Defendant's inadequate data security measure practices and/or omissions regarding its data security and privacy-related practices constitutes unlawful, deceptive, and unfair conduct in violation of the following State-specific consumer protection laws:

a. Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1522;

b. Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107–108;

c. California Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.*;

d. California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*;

e. Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-105(1);

f. Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. §§ 42-110b, *et seq.*;

g. Delaware Consumer Fraud Act, Del. Code Ann. tit. 6, §§ 2513, *et seq.*;

h. Delaware Deceptive Trade Practices Act, Del. Code Ann. Tit. 6, §§ 2532(5) and (7);

i. Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. §§ 480-2(a), *et seq.*;

j. Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7), and (12), *et seq.*;

k. Idaho Consumer Protection Act, Idaho Code Ann. §§ 48-603, *et seq.*;

l. Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. Ann. §§ 505/2, *et seq.*;

m. Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. Ann. §§ 510/2, *et seq.*;

n. Indiana Deceptive Consumer Sales Act, Ind. Code Ann. § 24-5-0.5-3(a), (b)(1), and (2), *et seq.*;

o. Iowa Consumer Fraud Act, Iowa Code §§ 714H.3 and 714H.5, *et seq.*;

p. Kansas Consumer Protection Act, Kan. Stat. Ann. § 50-626(a) and (b)(1)(A), (D) and (b)(3), *et seq.*;

q. Kentucky Consumer Protection Act, Ky. Rev. Stat. Ann. § 367.170(1) and (2), *et seq.*;

r. Maine Unfair Trade Practices Act, Me. Rev. Stat. Ann. tit. 5, § 207, *et seq.*;

s. Maine Uniform Deceptive Trade Practices Act, Me. Rev. Stat. Ann. tit. 10, § 1212(1)(E) and (G), *et seq.*;

t. Maryland Consumer Protection Act, Md. Code Ann. Com. Law, § 13-301(1), (2)(i)-(ii),(iv), (5)(i), and (9)(i), *et seq.*;

u. Massachusetts Consumer Protection Act, Mass. Gen. Laws ch. 93A, § 2(a), *et seq.*;

v. Michigan Consumer Protection Act, Mich. Comp. Laws Ann. § 445.903(1)(c), (e), (s), and (cc), *et seq.*;

w. Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7), and (13), *et seq.*;

x. Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(A);

y. Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. §§ 30-14-103;

z. Nebraska Consumer Protection Act, Neb. Rev. Stat. Ann. § 59-1602;

aa. Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. Ann. § 87-302(A)(5) and (7);

bb. New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(V) and (VII);

cc. New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2;

dd. New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7), (14), and 57-12-3;

ee. Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7);

ff. New York Business Law, N.Y. Gen. Bus. Law § 349(A);

gg. North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. Ann. § 75-1.1(A);

hh. North Dakota Unlawful Sales or Advertising Practices Law, N.D. Cent. Code § 51-15-02;

ii. Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2);

jj. Oklahoma Consumer Protection Act, Okla. Stat. Ann. § 753(5), (7), and (20);

kk. Oklahoma Deceptive Trade Practices Act, Okla. Stat. Ann. tit. 78, § 53(A)(5) and (7);

ll. Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(E), (G), and (U);

mm. Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. Ann. §§ 201-2(4)(V), (VII), (XXI), and 201-3;

nn. Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(V), (VII), (XII), (XIII), and (XIV);

oo. South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1);

pp. Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. & Com. Code Ann. § 17.46(A), (B)(5) and (7);

qq. Utah Consumer Sales Practices Act, Utah Code Ann. § 13-11-4(1) and (2)(A), (B), and (I);

rr. Vermont Consumer Fraud Act, 9 Vt. Stat. Ann. Tit. 9, § 2453(A);

ss. Washington Consumer Protection Act, Wash. Rev. Code RCW §§ 19.86.010, *et seq.*;

tt. West Virginia Consumer Credit and Protection Act, W. Va. Code Ann. § 46A-6-104; and

uu. Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii), and (xv).

203. As a result of Defendant's conduct, Plaintiffs and members of the Statewide Statutory Classes have suffered actual damages, including from the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of

identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

204. Accordingly, Plaintiffs, on behalf of themselves and members of the Statewide Statutory Classes, seek to enjoin further violation and recover actual damages (and treble damages where applicable).

205. With respect to injunctive relief, Plaintiffs, on behalf of themselves and members of the Statewide Statutory Classes, seek an Order requiring Premera to: (1) engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Premera's systems on a periodic basis, and ordering Premera to promptly correct any problems or issues detected by such third-party security auditors; (2) engage third-party security auditors and internal personnel to run automated security monitoring; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) segment data by, among other things, creating firewalls and access controls so that if one area of Premera's network is compromised, hackers cannot gain access to other portions of Premera's systems; (5) purge, delete, and destroy in a reasonably secure manner Sensitive Information not necessary for its provisions of services; (6) conduct regular database scanning and securing checks; (7) routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it

occurs and what to do in response to a breach; and (8) meaningfully educate all class members about the threats they face as a result of the loss of their confidential financial, personal, and health information to third parties, as well as the steps affected individuals must take to protect themselves.

EIGHTH CLAIM FOR RELIEF
Violation of State Data Breach Notification Laws
(*In the alternative to Second Claim for Relief*)
(On behalf of Plaintiffs and the Statewide Statutory Classes)

206. Plaintiffs incorporate all the foregoing factual allegations as if fully set forth herein, excluding paragraphs 140-144.

207. Plaintiffs allege additionally and alternatively that the data breach notification laws listed below were enacted to protect (or at least mitigate damage for) consumers from the consequences associated with data breaches. In relevant part, those laws require that businesses that maintain consumer data (including Sensitive Information) notify the owner of any breach of that data in the most expedient time and manner possible and without unreasonable delay.

208. The data breach described in Section II resulted in a breach of Plaintiffs' and the Statewide Statutory Class members' Sensitive Information.

209. Defendant failed to disclose the breach of Plaintiffs' and the Statewide Statutory Class members' Sensitive Information in the most expedient time possible inasmuch as, after discovering the breach, it waited months before notifying all affected individuals. Defendant unreasonably delayed informing Plaintiffs and members of the Statewide Statutory Class about the data breach after it knew or should have known that the data breach had occurred.

210. Defendant's failure to provide timely notice of the data breach violated the following State-specific data breach notification laws:

a) Cal. Civ. Code § 1798.80, *et seq.*;

b) Ill. Comp. Stat. Ann. 530/10, *et seq.*;

c) Iowa Code Ann. § 715C.2, *et seq.*;

d) La. Rev. Stat. Ann. § 51:3074, *et seq.*;

e) Md. Code Ann., Commercial Law § 14-3504, *et seq.*;

f) N.H. Rev. Stat. Ann. § 359-C:20, *et seq.*;

g) N.J. Stat. Ann. § 56:8-163, *et seq.*;

h) N.C. Gen. Stat. Ann. § 75-65, *et seq.*;

i) S.C. Code § 39-1-90, *et seq.*;

j) Tenn. Code Ann. § 47-18-2107, *et seq.*;

k) Tex. Bus. & Com. Code Ann. § 521.053, *et seq.*; and

l) Va. Code Ann. § 18.2-186.6, *et seq.*;

211. As a result of Defendant's conduct, Plaintiffs and members of the Statewide Statutory Class have suffered actual damages, including from the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the

deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

212. Accordingly, Plaintiffs, on behalf of themselves and members of the Statewide Statutory Class, seek all remedies available under their state data breach statute, including but not limited to (a) damages suffered by Plaintiffs and the Statewide Statutory Class members as alleged above, (b) equitable relief, including injunctive relief, and (c) reasonable attorney fees and costs, as provided by law.

NINTH CLAIM FOR RELIEF
Violation of the California Confidential Medical Information Act
(On behalf of Plaintiff Hansen-Bosse and the Statewide California Statutory Class)

213. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

214. Plaintiffs allege additionally and alternatively that California's Confidential Medical Information Act was enacted to protect, among other things, the release of confidential medical information without proper authorization. *See* Confidential Medical Information Act, Cal. Civ. Code §§ 56, *et seq.* ("CMIA"). To that end, the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information. *See* Cal. Civ. Code § 56.36 (2013). The CMIA also requires that an entity, such as Defendant, that "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Civ. Code § 56.101(a).

215. As described throughout this Complaint, Defendant negligently disclosed and released Plaintiffs' and the Statewide California Subclass members' Sensitive Information

inasmuch as it did not implement adequate security protocols to prevent unauthorized access to Sensitive Information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data breach or otherwise comply with HIPAA data security requirements.

216. As a direct and proximate result of Defendant's negligence, it disclosed and released Plaintiffs' and the Statewide California Statutory Class members' Sensitive Information to hackers.

217. Accordingly, Plaintiffs, on behalf of themselves and members of the Statewide California Statutory Class, seek to recover actual, nominal (including $1000 nominal damages per disclosure under § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

TENTH CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Nationwide Data Breach Class or, alternatively, the Statewide Common Law Classes)

218. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

219. In requiring Plaintiffs and Nationwide Data Breach Class members or, alternatively, members of the Statewide Common Law Classes, to submit Sensitive non-public personal health and financial information in order to obtain coverage under a health insurance policy and/or receive treatment in the Blue Cross Blue Shield network, Premera placed itself in a position trust with respect to such Sensitive non-public personal health and financial information.

220. This position of trust was enhanced by Premera's necessary involvement in the fiduciary relationship between doctors and their patients, and by Premera's own fiduciary or quasi-fiduciary relationship as an insurer to its insured.

221. Premera's position of trust arises under HIPAA, pursuant to which Premera is required to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

222. In addition Premera's position of trust is enhanced by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by healthcare benefit providers like Defendant. The FTC publications and data security breach orders described above further form the basis of Premera's duty.

223. As guardians of Sensitive non-public personal health and financial information, Premera owed a fiduciary duty to Plaintiffs and Nationwide Data Breach Class members or, alternatively, members of the Statewide Common Law Classes, to secure and safeguard this personal and health information, to prevent disclosure of the information, and to guard the information from theft. Premera's fiduciary duty included the duty to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give immediate notice of a data breach.

224. Premera breached its fiduciary duty by failing to use sufficient measures to protect consumers' confidential data from hackers and by failing to provide timely notice of the at-issue breach. The specific acts and omissions committed by Premera include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and proposed Nationwide Data Breach Class members' or alternatively, members of the Statewide Common Law Classes' confidential data;

b. Failing to monitor the security of its networks adequately;

c. Allowing unauthorized access to Plaintiffs' and the proposed Nationwide Data Breach Class members' or, alternatively, members of the Statewide Common Law Classes' confidential data;

d. Failing to recognize in a timely manner that Plaintiffs' and proposed Nationwide Data Breach Class members' or alternatively, members of the Statewide Common Law Classes' confidential data had been compromised; and

e. Failing to warn Plaintiffs and the members of the proposed Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes in a timely manner that their Sensitive Information was likely to be and had been compromised.

225. It was foreseeable that Premera's failure to use sufficient measures to protect confidential data, to disclose to Plaintiffs its inadequate security system and to provide timely notice of a breach of such data would result in injury to Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes were foreseeable, particularly in light of the other major data breaches affecting the healthcare industry and the warning provided by federal auditors (described in Section I, above) that Premera's network-security procedures were inadequate and that the vulnerabilities could be exploited by hackers and expose sensitive information.

226. It was therefore reasonably foreseeable that the failure to safeguard confidential data adequately would result in one or more of the following injuries to Plaintiffs and the members of the proposed Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

227. Accordingly, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, seek an order declaring that Defendant's conduct constitutes breach of fiduciary duty, and awarding them damages in an amount to be determined at trial.

228. Washington law should apply to the breach of fiduciary duty claim of the Nationwide Class, or, alternatively, the negligence claims of the Statewide Common Law Classes should be governed by the law of each state in which such state specific claims are brought.

ELEVENTH CLAIM FOR RELIEF
Misrepresentation by Omission
(On behalf of Plaintiffs and the Nationwide Data Breach Class or, alternatively, the Statewide Common Law Classes)

229. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

230. Premera knew or should have known that it failed to use sufficient measures to protect consumers' confidential data from hackers as described above.

231. Premera fraudulently, negligently, or recklessly concealed from, or failed to disclose to, the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, the fact that the measures it employed to protect consumers' confidential data from hackers were insufficient.

232. Premera was under a duty to the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, to disclose the insufficient nature of its security measures because: 1) Premera was in a superior position to know the true state of the facts about the design of its security measures because the design of such security measures is not public; 2) Premera stands in a fiduciary or quasi fiduciary relationship with its insureds; and 3) Premera made partial disclosures about maintaining the confidentiality of confidential data without revealing that it had taken insufficient measures to protect that information from hackers.

233. The facts not disclosed to the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, are material facts in that a reasonable person would have considered those facts to be important in deciding whether or not to purchase insurance through Premera. Had the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, known the insufficient nature of Premera's security measures, they would not have purchased insurance through Premera or would have paid less for it.

234. Premera intentionally, recklessly, or negligently concealed or failed to disclose the insufficient nature of its security measures for the purpose of inducing the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, to act thereon, and the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, justifiably relied to their detriment upon the truth and completeness of Premera's representations. This is evidenced by the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, purchase of insurance through Premera.

235. As a direct and proximate cause of Premera's misconduct, the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, have suffered and will continue to suffer actual damages in ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and the difference in the free-market value of the secure healthcare insurance for which they paid and the insecure healthcare insurance they received.

236. Accordingly, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, seek an order declaring that Defendant's conduct constitutes a misrepresentation, and awarding them damages in an amount to be determined at trial.

237. Washington law should apply to a misrepresentation claim of the Nationwide Class, or, alternatively, the negligence claims of the Statewide Common Law Classes should be governed by the law of each state in which such state specific claims are brought.

VII. REQUEST FOR RELIEF

Plaintiffs, on behalf of themselves and the Classes, respectfully request that this Court enter an Order:

A. Certifying this case as a class action on behalf of Plaintiffs and the Classes defined above, appointing Plaintiffs as representatives of their respective Classes, and appointing Interim Lead Counsel as Class Counsel;

B. Declaring that Premera's actions, as described above, constitute violations of the Washington Consumer Protection Act; Washington Data Breach Disclosure law; Negligence; Breach of Express Contract; Breach of Implied Contract; Restitution/Unjust Enrichment; violations of the consumer protection laws of Arizona, Arkansas, California, Connecticut, Idaho, Illinois, Kansas, Kentucky, Maryland, Massachusetts, New Jersey, Oregon, and Texas; violations of the data breach notification laws of California, Illinois, Maryland, New Jersey, Tennessee, and Texas; and violations of the California Confidential Medical Information Act.

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Classes, including (i) an order prohibiting Premera from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Premera to protect all data collected through the course of its business in accordance with HIPAA regulations, federal, state and local laws, and industry standards; (iii) requiring Premera to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Premera's systems on a periodic basis, and

ordering Premera to promptly correct any problems or issues detected by such third-party security auditors; (iv) requiring Premera to engage third-party security auditors and internal personnel to run automated security monitoring; (v) requiring Premera to audit, test, and train its security personnel regarding any new or modified procedures; (vi) requiring Premera to segment data by, among other things, creating firewalls and access controls so that if one area of Premera's network is compromised, hackers cannot gain access to other portions of Premera's systems; (vii) requiring Premera to purge, delete, and destroy in a reasonably secure manner Sensitive Information not necessary for its provisions of services; (viii) requiring Premera to conduct regular database scanning and securing checks; (ix) requiring Premera to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (x) requiring Premera to meaningfully educate all class members about the threats they face as a result of the loss of their confidential financial, personal, and health information to third parties, as well as the steps affected individuals must take to protect themselves.

D. Awarding actual, statutory, exemplary and punitive damages to Plaintiffs and the Classes, where applicable, in an amount to be determined at trial;

E. Awarding restitution to Plaintiffs and the Classes in an amount to be determined at trial;

F. Awarding Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

G. Awarding Plaintiffs and the Classes pre- and post-judgment interest, to the extent allowable;

H. Permitting Plaintiffs and the Classes to amend their pleadings to conform to the evidence produced at trial; and

I. Awarding such other and further relief as equity and justice may require.

VIII. JURY DEMAND

Plaintiffs request a trial by jury.

Respectfully submitted,

TOUSLEY BRAIN STEPHENS, PLLC

Dated: October 6, 2015

By: *s/ Kim D. Stephens*

Kim D. Stephens, OSB No. 030635
Christopher I. Brain, admitted *pro hac vice*
Chase C. Alvord, OSB No. 070590
Jason T. Dennett, admitted *pro hac vice*
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
Email: cbrain@tousley.com
kstephens@tousley.com
calvord@tousley.com
jdennett@tousley.com

Interim Lead Plaintiffs' Counsel

STOLL STOLL BERNE LOKTING & SHLACHTER P.C.

By: *s/ Keith S. Dubanevich*

Keith S. Dubanevich, OSB No. 975200
Steve D. Larson, OSB No. 863540
Mark A. Friel, OSB No. 002592
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840
Email: kdubanevich@stollberne.com
slarson@stollberne.com
mfriel@stollberne.com

Interim Liaison Plaintiffs' Counsel

Ari J. Scharg
ascharg@edelson.com
EDELSON PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Tina Wolfson
twolfson@ahdootwolfson.com
AHDOOT AND WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069
Tel: 310.474.9111
Fax: 310.474.8585

James Pizzirusso
jpizzirusso@hausfeldllp.com
HAUSFELD LLP
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: 202.540.7200
Fax: 202.540.7201

Plaintiffs' Executive Leadership Committee

CERTIFICATE OF SERVICE

I hereby certify that on this day I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all counsel of record.

s/ Steve D. Larson
Steve D. Larson